Information and Computation 210 (2012) 13–20

Contents lists available at SciVerse ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

On Ladner's result for a class of real machines with restricted use of constants

Klaus Meer

Computer Science Institute, BTU Cottbus, Konrad-Wachsmann-Allee 1, D-03046 Cottbus, Germany

ARTICLE INFO

Article history:
Received 10 June 2010
Revised 28 October 2011
Available online 6 November 2011

Keywords:
Complexity
Real number model
Diagonal problems
Ladner's theorem

ABSTRACT

We study the question whether there are analogues of Ladner's result in the computational model of Blum, Shub and Smale. It is known that in the complex and the additive BSS model a pure analogue holds, i.e. there are non-complete problems in $\mathrm{NP} \setminus \mathrm{P}$ assuming $\mathrm{NP} \neq \mathrm{P}$. In the (full) real number model only a non-uniform version is known. We define a new variant which seems relatively close to the full real number model. In this variant inputs can be treated as in the full model whereas real machine constants can be used in a restricted way only. Our main result shows that in this restricted model Ladner's result holds. Our techniques analyze a class P/const that has been known previously to be crucial for this kind of results. By topological arguments relying on the polyhedral structure of certain sets of machine constants we show that this class coincides with the new restricted version of $\mathrm{P}_{\mathbb{R}}$, thus implying Ladner's result.

1. Introduction

Ladner's result [8] states that assuming $\mathrm{P} \neq \mathrm{NP}$ there exist problems in $\mathrm{NP} \setminus \mathrm{P}$ which are not NP-complete under polynomial-time many-one reductions. The respective question has been studied in other models as well. For Valiant's complexity classes VP and VNP a Ladner like result was shown in [3]. In the computational model introduced by Blum, Shub, and Smale several similar results have been proved. For the BSS model over the complex numbers Ladner's result holds analogously [9]. In [1] the authors analyzed how far this result can be extended to further structures. They showed that a class P/const is of major importance for such questions. P/const was introduced by Michaux [11]. It denotes all decision problems that can be solved non-uniformly by a machine $M(x, c)$ that has a constant number k of non-rational machine constants $c \in \mathbb{R}^k$ and runs in polynomial time. M solves the problem up to input dimension n by taking for each n non-uniformly a potentially new set of constants $c^{(n)} \in \mathbb{R}^k$. For a more precise definition see below. It turns out that if $\mathrm{P} = \mathrm{P/const}$ in a structure in which quantifier elimination is possible, then Ladner's result holds in this structure. The latter is the case for $\mathbb{C}$ as well as for $\{0, 1\}^*$. Over the reals it is unknown whether (and in fact unlikely that) $\mathrm{P}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}/\mathrm{const}$. The currently strongest known version of a Ladner like result in the full BSS model over $\mathbb{R}$ is the following non-uniform statement: If $\mathrm{NP}_{\mathbb{R}} \not\subseteq \mathrm{P}_{\mathbb{R}}/\mathrm{const}$, then there are problems in $\mathrm{NP}_{\mathbb{R}} \setminus (\mathrm{P}_{\mathbb{R}}/\mathrm{const})$ which are not $\mathrm{NP}_{\mathbb{R}}$-complete [1]. Chapuis and Koiran [5] give a deep model-theoretic analysis of real complexity classes of the form $\mathcal{C}/\mathrm{const}$ relating them to the notion of saturation. As a by-product of their investigations they obtain Ladner's result for the reals with order and addition.

The present paper continues this line of research. In order to come closer to a complete analogue of Ladner's result in the full real number model we introduce a new variant of it that has to the best of our knowledge not been studied so far. This variant has full access to the input data but limited access to real machine constants. More precisely, an algorithm that uses machine constants $c_1, \ldots, c_k \in \mathbb{R}$ and gets an input $x \in \mathbb{R}^n$ is allowed to perform any operation among $\{+, -, *\}$ if an x_i

E-mail address: meer@informatik.tu-cottbus.de.

0890-5401/$ – see front matter
doi:10.1016/j.ic.2011.11.001

is involved as operand. Two operands involving some of the c_i's can only be combined by $+$ or $-$. We call this model real number model with restricted use of constants. Its deterministic and non-deterministic polynomial time complexity classes are denoted by $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ and $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$, respectively. More details are given in Section 2. In a certain sense this variant swaps the roles inputs and machine constants are playing in the linear BSS model [2]. Whereas in the latter all computed results depend linearly on the inputs but arbitrarily on machine constants, in the new variant it is just the opposite. However, this analogy is not complete since in our variant the degrees of intermediate results as polynomials in the input components can still grow exponentially in the number of computation steps, something that is not true in the linear BSS model with respect to the constants.

It turns out that the new variant is somehow closer to the full BSS model than other variants studied so far. For example, we show that some $\mathrm{NP}_{\mathbb{R}}$-complete problems are as well complete in $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$.[1] The present paper investigates an analogue of Ladner's theorem in the restricted model. Towards this aim we start from the results in [1]. The main task is to analyze the corresponding class $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ and to show on the one side that the diagonalization technique developed in [1] can be applied to $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ as well. On the other side the more difficult part will be to show that $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ actually is contained—and thus equal to—the class $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$. As a main contribution of the paper we show equality of the two classes:

Theorem 1. *We have* $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const} = \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$.

By standard arguments well known in the field this implies Ladner's result in the restricted model:

Theorem 2. *Assuming FEAS* $\notin \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ *for the* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$*-complete problem FEAS in the BSS model with restricted use of constants there exist problems in* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}} \setminus \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ *which are not* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$*-complete.*

Here, FEAS denotes the $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete problem to decide whether a system of quadratic polynomial equations has a common real zero, see below.

The paper is organized as follows. Section 2 recalls previous results including necessary definitions of the models and complexity classes we are interested in. We introduce the restricted variant of the real number model. It is then shown that the $\mathrm{NP}_{\mathbb{R}}$-complete problem of deciding solvability of a system of real polynomial equations as well belongs to $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$ and is complete in this class under $\mathrm{FP}_{\mathbb{R}}^{\mathrm{rc}}$-reductions. The diagonalization technique from [1] is then shown to work for $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ as well. In Section 3 the main result, namely the relation $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const} \subseteq \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ is established. It implies the analogue of Ladner's theorem for $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$. The paper finishes with some discussions.

An extended abstract of this paper has appeared in [10].

2. Basic notions and first results

We suppose the reader to be familiar with the BSS model over the reals [2]. Very briefly, a BSS machine is a uniform Random Access Machine that computes with real numbers as basic entities. An input $x \in \mathbb{R}^n$ is given the algebraic size $size_{\mathbb{R}}(x) := n$, and each operation $\{+, -, *, :, \geqslant 0?\}$ among real numbers can be performed with (algebraic) costs 1. The complexity class $\mathrm{P}_{\mathbb{R}}$ consists of all decision problems $L \subseteq \mathbb{R}^* := \bigcup_{i \geqslant 1} \mathbb{R}^i$ for which there exists a polynomial time BSS algorithm deciding membership in L. The class $\mathrm{NP}_{\mathbb{R}}$ contains a set L iff there exists a polynomial time verification procedure that satisfies the following requirements. Given $x \in L$ there is a proof y of polynomial length in the (algebraic) size of x such that the procedure accepts (x, y). And for every $x \notin L$ the procedure rejects all tuples (x, y), no matter how y looks like.

In this paper we deal with a variant of the BSS model (and the above complexity classes) which results from restricting the way in which algorithms are allowed to use real machine constants.

Definition 1.

a) Let A be a BSS algorithm using $c_1, \ldots, c_k$ as its non-rational machine constants. Here $k \in \mathbb{N}$ is a constant only depending on A. An intermediate result computed by A on input x from some $\mathbb{R}^n$ is called *marked* if it, as a function of (x, c), depends on at least one of the c_i's, otherwise it is *unmarked*.
b) The *real number model with restricted use of constants* is the variant of the full BSS model in which the following condition is imposed on usual BSS algorithms. A *restricted* machine can perform the operations $\{+, -, *\}$ if at least one operand is unmarked. If both operands are marked, it can perform $+$ and $-$ only. For an intermediate result t tests of the form 'is $t \geqslant 0$?' can be performed on both kind of operands.
c) The cost of a restricted algorithm is defined as in the full model, i.e. each operation counts one. We denote the resulting analogues of $\mathrm{P}_{\mathbb{R}}$ and $\mathrm{NP}_{\mathbb{R}}$ by $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ and $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$, respectively.

[1] Though this is true as well for Koiran's weak model its different cost measure implies dramatic differences to the full model because $P \neq NP$ has been proved in the former [6].

A few remarks should clarify the power and the limits of the restricted model. We do not include divisions by unmarked operands for sake of simplicity. This would not change anything significantly. The condition on how to differentiate between marked and unmarked intermediate results guarantees a certain control on how real machine constants influence the results. More precisely, such an algorithm can compute arbitrarily with input components, whereas machine constants only occur linearly. Thus, each value computed by a restricted algorithm on an input $x \in \mathbb{R}^n$ is of the form $\sum_{i=1}^k p_i(x) \cdot c_i + q(x)$. Here, the p_i's and q are polynomials in the input with rational coefficients. Contrary to for example the weak model introduced by Koiran the degrees of these polynomials still can grow exponentially in polynomial time. For rational machine constants no condition applies, i.e. they can be used arbitrarily. As a potential limit of the restricted model note that when composing machines, constants of the first might become inputs of the second algorithm. Thus it is unclear whether reductions can be composed in general. Nevertheless, as we shall see below this problem has no significant impact for our purposes since there exist $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete problems.

A typical example of a problem solvable efficiently by an algorithm in $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ is the following: Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ and a $y \in \mathbb{R}^n$, is $f(y) = 0$? Here, f is given by the coefficients of its monomials. Both these coefficients and y are inputs to the problem, so the normal evaluation algorithm does not need additional constants. All of its operations can be performed by a restricted algorithm. Arguments of this kind shall be used again below to prove existence of complete problems. Another example takes as input a polynomial f as above and asks whether f has a real zero all of whose components can be found among the components of a real zero of a fixed real polynomial g. This problem is in $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$. Guess a zero y of g and a zero z of f such that all of z's components are among those of y. Evaluation of f in z is done as above, evaluation of g in y needs g's coefficients as machine constants. However, they only occur restrictedly in the evaluation procedure.

The study of transfer results of the P versus NP question between different structures led Michaux to the definition of the complexity class P/const [11]. It is a non-uniformly defined class which allows a uniform polynomial time machine to use non-uniformly different choices of machine constants for different input dimensions. Below we change a bit Michaux' original definition with respect to two technical details. We split rational uniform constants and potentially real constants that might be changed for each dimension. And we require the real machine constants to be bounded in absolute value by 1. Both changes do not affect the results from [1] as we are going to show later.

Definition 2. A *basic machine over* $\mathbb{R}$ in the BSS-setting is a BSS-machine M with rational constants and with two blocks of input variables, one block x taking values in $\mathbb{R}^\infty$, the other one c taking values in some $\mathbb{R}^k \cap [-1, 1]^k$ ($k \in \mathbb{N}$ fixed for M). Here $\mathbb{R}^\infty := \bigcup_{n \geqslant 1} \mathbb{R}^n$ denotes the set of all finite sequences of real numbers.

Basic machines for the restricted model are defined similarly.

The above definition of a basic machine intends to split the discrete skeleton of an original BSS machine from its real machine constants. That is done by regarding those constants as a second block of parameters. Fixing c we get back a usual BSS machine $M(\bullet, c)$ that uses c as its constants for all input instances x. If below we speak about the machine's constants we refer to the potentially real ones only.

Definition 3. (Cf. [11].) A problem L is in class $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$*/const* if and only if there exists a restricted polynomial time basic machine M and for every $n \in \mathbb{N}$ a tuple $c^{(n)} \in [-1, 1]^k$ of real constants for M such that $M(\bullet, c^{(n)})$ decides L up to size n.

An easy result needed below is the following.

Lemma 3. *We have* $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}} \subseteq \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$.

Proof. Let $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ and M be a restricted machine for L. M can be seen as basic machine proving $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ if all its constants are in $[-1, 1]$. However, if a constant $r \in \mathbb{R}$ is larger in absolute value we can decompose it into $r_1 + r_2$ with integral r_1 and $|r_2| \leqslant 1$. Since basic machines are allowed to use arbitrarily rational uniform constants this gives a new restricted machine for L which uses real constants in $[-1, 1]$ only. $\square$

In a number of computational models the class P/const has strong relations to Ladner's result. In [1] the authors show for a number of structures including $\mathbb{R}, \mathbb{C}$ and finite structures that if $\mathrm{NP} \not\subseteq \mathrm{P}/\mathrm{const}$ there are problems in $\mathrm{NP} \setminus (\mathrm{P}/\mathrm{const})$ that are not NP-complete. Michaux proved in [11] that for recursively saturated structures $\mathrm{P} = \mathrm{P}/\mathrm{const}$. As consequence the result mentioned above reproves Ladner's result both for the Turing model [8] and the BSS model over $\mathbb{C}$ [9]. Over the reals the currently strongest Ladner like theorem is the following.

Theorem 4. *(See [1].) Suppose* $\mathrm{NP}_{\mathbb{R}} \not\subseteq \mathrm{P}_{\mathbb{R}}/\mathrm{const}$. *Then there exist problems in* $\mathrm{NP}_{\mathbb{R}} \setminus (\mathrm{P}_{\mathbb{R}}/\mathrm{const})$ *not being* $\mathrm{NP}_{\mathbb{R}}$*-complete under polynomial-time many-one reductions.*

Concerning a further analysis of $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$ and its relation to uniform classes, in particular to $\mathrm{P}_{\mathbb{R}}$, not much is known. Chapuis and Koiran [5] argue that already $\mathrm{P}_{\mathbb{R}}/1 = \mathrm{P}_{\mathbb{R}}$ is unlikely; here, $\mathrm{P}_{\mathbb{R}}/1$ is defined by means of basic machines which use a finite number of uniform and a single non-uniform machine constant only.

The main result below shows that the same line of arguments used in [1] extends to the restricted model as well. The way it is obtained might also shed new light on what can be expected for the full model. Some ideas are discussed in the conclusion section.

2.1. Complete problems in $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$

An indication for our earlier remark that the restricted model is not too exotic is to show that it shares complete problems with the original BSS model. Beside showing this the result given below is also needed with respect to the quantifier elimination procedure in the next subsection. The main point here is that such an elimination can be performed as well by a restricted machine. Towards this goal it is necessary to establish completeness of problems that do not involve non-rational constants.

Theorem 5. *The feasibility problem FEAS which asks for solvability of a system of real polynomial equations of degree at most two is $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete in the BSS model with restricted use of machine constants.*

Proof. The problem *FEAS* belongs to $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$. Given such a system by coding the coefficients of each monomial of the single polynomial equations a verification algorithm guesses as usual a potential real solution and evaluates all polynomials in the guessed point. Since both the coefficients and the potential solution are inputs for this algorithm it does not need any real constants and thus can be performed by making restricted use of constants.

For $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-completeness we only have to check the usual $\mathrm{NP}_{\mathbb{R}}$-completeness proof of *FEAS* from [2]. Here, the reduction of a computation of an $\mathrm{NP}_{\mathbb{R}}$-machine M on an input x to the feasibility question of a polynomial system takes x as input. It then introduces for each step new variables which in a suitable way reflect the computation done in this step. To make the argument as easy as possible we can require that a (restricted) reduction algorithm at the very beginning introduces for each real constant c_i which M is using a new variable z_i together with the equation $c_i = z_i$ and then only uses z_i. The resulting polynomial system is constructed without additional real constants beside the c_i's. Moreover this construction algorithm uses the c_i's only in the demanded restricted way. $\square$

2.2. Diagonalization between $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ and $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$

As first result we shall prove that an analogue version of Theorem 4 is as well true in the restricted model.

Theorem 6. *Suppose FEAS* $\notin \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ *(and thus* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}} \not\subseteq \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$*). Then there exists a problem L in* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}} \setminus (\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const})$ *not being* $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$*-complete under restricted polynomial time many-one reductions.*

Proof. In order to avoid a word-by-word repetition of [1] we just elaborate the main new arguments. We suppose therefore the reader to be familiar with Ladner's padding argument and below just briefly recall the main idea of the proof of Theorem 4 as it used here. It relies on the fact that the set of basic machines over $\mathbb{R}$ is countable together with a variant of the typical padding argument used by Ladner. Starting from an $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete problem the goal is to define a problem L that satisfies the theorem's statement by changing the complete problem on certain input dimensions to be an easy problem. The definition of those dimensions where L looks as the original problem and those where it looks easy is done in such a way that at the same time both all $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ machines and all potential $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ reductions from the given complete problem to L work erroneously. Towards this goal for each basic machine (either one realizing an $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ algorithm or one realizing a reduction) a suitable "fooling" dimension is searched. The crucial point here is that such dimensions are computable due to the existence of quantifier elimination algorithms. In order to transfer the proof of Theorem 4 to $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ it is thus necessary to show the following: We can describe the existence of error dimensions by a quantified first-order formula in the theory of the reals. And this dimension can be effectively computed by eliminating the quantifiers with a restricted machine. Especially the latter point requires a bit more care.

Consider the $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete problem *FEAS*. By assumption it is not in $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$. We describe the definition of the problem L together with the computation of a suitable error dimension for potential polynomial time decision algorithms. The argument for fooling polynomial time reduction algorithms is basically the same, the mixture of the two arguments in order to fulfill as well the complexity requirements is standard, see [8,1].

Let M denote a basic restricted polynomial time machine using k constants. Suppose L has already been defined up to a dimension m; the next goal is to extend the definition of L up to a dimension $n_M > m$ such that M will fail to decide L correctly for an input of dimension $\leqslant n_M$. On inputs of dimension larger than m we let L look like the problem *FEAS* in order to guarantee that an appropriate dimension n_M must exist. The key point is to show that such an n_M can be computed as well.

For each input dimension $n \in \mathbb{N}$ we can construct a first order formula in the theory of the reals saying the following: There is no choice of constants from $\mathbb{R}^k$ that can be used by M in order to decide $L \cap \mathbb{R}^{\leqslant n}$ correctly. This formula is obtained as follows, see [1]: First, since $FEAS \in \mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$ for every n there is a first-order formula $\rho_n(x)$ defining the restriction of L to $\mathbb{R}^{\leqslant n}$. The particular form of the problem guarantees $\rho_n(x) \equiv \exists y \tilde{\rho}_n(x, y)$, where $\tilde{\rho}$ has no non-rational constants. Secondly, the computation of M on inputs of dimension at most n using machine constants $c \in \mathbb{R}^k$ can be described by a first-order formula $\Phi_n(x, c)$. Since M is a restricted machine Φ_n depends linearly on the components of c and has no other non-rational constants. Thirdly, the sentence

$$\Theta_n \equiv \forall c \in [-1,1]^k \; \exists x \in \mathbb{R}^{\leqslant n} \; \neg\big(\Phi_n(x,c) \Leftrightarrow \rho_n(x)\big)$$

is true iff the set $E_n \subseteq \mathbb{R}^k$ of constants that can be used by M to decide $L \cap \mathbb{R}^{\leqslant n}$ is empty. This is equivalent to saying that M does not witness $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$. Now for every n we can decide the truth of the above formula Θ_n by eliminating quantifiers. It is necessary that the elimination can be performed by a restricted machine. This is possible because first an elimination procedure like Tarski's does not introduce new constants and secondly there are only rational constants present in Θ_n. Thus we can compute effectively by a restricted machine for every basic machine M a dimension n_M on which M fails to witness $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$. The same arguments apply for $\mathrm{FP}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ reduction machines. We are then again in the scope of the proof of Theorem 4 and the claim follows. □

3. Proof of the main results

In this section we shall show Theorem 1 thus implying Ladner's result in the BSS model with restricted use of constants. Since the proof is a bit involved let us first outline the main ideas. Let $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ and M be a corresponding basic machine establishing this membership. Suppose M uses k machine constants. The overall goal is to find, by means of an algorithm that is uniform in n, for each dimension n a suitable choice of constants that could be used by M to decide $L \cap \mathbb{R}^{\leqslant n}$. We suppose that there is no uniform choice of one set of constants working for M; otherwise $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ is a trivial consequence and nothing is left to be shown.

Let $E_n \subseteq [-1,1]^k$ denote the suitable constants working for $L \cap \mathbb{R}^{\leqslant n}$ when used by M. Thus, for $x \in \mathbb{R}^{\leqslant n}$ we ideally would like to find efficiently and uniformly a $c^{(n)} \in E_n$ and let then run M on $(x, c^{(n)})$.[2] However, we shall not compute such a $c^{(n)}$. Instead we shall show that there are three vectors $c^*, d^*, e^* \in \mathbb{R}^k$ such that for all dimensions $n \in \mathbb{N}$ if we move a short step (depending on n) from c^* into the direction of d^* and afterwards a short step into the direction e^* we end up in E_n. This argument is relying on the topological structure of the E_n's and given in Section 3.1. We are then left with deciding an assertion of the following structure:

$$\begin{aligned}&\forall n \in \mathbb{N}\; \exists \epsilon_1 > 0\; \forall \mu_1 \in (0,\epsilon_1)\; \exists \epsilon_2 > 0\; \forall \mu_2 \in (0,\epsilon_2)\; M \text{ works correctly on } \mathbb{R}^{\leqslant n}\\ &\quad \text{using as constants the vector } c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^*.\end{aligned}$$

In a second (easy) step we show that in the model with restricted use of constants statements of the above form can be decided efficiently.

3.1. Finding the correct directions

For $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ and M a suitable basic machine using k constants define

$$E_n := \big\{c \in [-1,1]^k \;\big|\; M(\bullet, c) \text{ correctly decides } L \cap \mathbb{R}^{\leqslant n}\big\} \subseteq [-1,1]^k.$$

M witnesses membership of L in $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$, so $E_n \neq \emptyset \; \forall n \in \mathbb{N}$. Without loss of generality suppose $\bigcap_{n=1}^{\infty} E_n = \emptyset$, otherwise $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ follows. The following facts about the sets E_n hold:

- for all $n \in \mathbb{N}$ it is $E_{n+1} \subseteq E_n$;
- none of the E_n is finite since otherwise there exists an index m with $E_m = \emptyset$;
- each E_n is a finite union of convex sets. Each of these convex sets is a (potentially infinite) intersection of open or closed halfspaces. This is true since for every n membership in E_n can be expressed by a formula resulting from writing down the behavior of M on inputs from $\mathbb{R}^{\leqslant n}$ when using a correct vector of constants from E_n. All computed intermediate results are of the form $\sum_{i=1}^{k} p_i(x) \cdot c_i + q(x)$, where p_i, q are polynomials. Thus, the tests produce for each x an open or closed halfspace with respect to suitable choices of c. If finitely many x are branched along a path only this results in a polyhedron, otherwise we obtain an infinite intersection of such halfspaces;
- nestedness and being a finite union of convex sets hold as well for the closures $\overline{E_n}$;
- each $\overline{E_n}$ has a finite number of connected components. This follows from the fact that the E_n are finite unions of convex and thus connected sets. Note that $\overline{E_n}$ is obtained from E_n by relaxing strict inequalities to non-strict ones.

[2] This is actually done in [5] to show that in the additive BSS model $\mathrm{P}_{\mathbb{R}}^{add}/\mathrm{const} = \mathrm{P}_{\mathbb{R}}^{add}$.

Now apply as in [5] König's infinity lemma (cf. [7]) to the infinite tree which has as its nodes on level n the connected components of E_n. The nestedness of the E_n (and thus of its connected components) implies that there is an $s \geqslant 1$, $s \leqslant k$ and a nested sequence of convex sets in $[-1,1]^k \cap E_n$ each of dimension s such that they have empty intersection. The inequality $s \geqslant 1$ follows because the E_n are non-finite. For notational simplicity we denote this nested sequence of sets again by $\{E_n\}_n$.

As first main result we show:

Theorem 7. *For the family $\{E_n\}_n$ of convex connected sets as defined above there exist vectors $c^*, d^*, e^* \in \mathbb{R}^k$ such that*

$$\forall n \in \mathbb{N}\ \exists \epsilon_1 > 0\ \forall \mu_1 \in (0,\epsilon_1)\ \exists \epsilon_2 > 0\ \forall \mu_2 \in (0,\epsilon_2):\quad c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^* \in E_n.$$

Proof. Let $\{E_n\}_n$ be as above and $\overline{E_n}$ the closure of E_n. Both are of dimension $s \geqslant 1$. Since each $\overline{E_n}$ is an intersection of halfspaces it is contained in an affine subspace of dimension $s \geqslant 1$. Now E_n is convex and therefore contains a polyhedron of dimension s. Let S be the affine subspace of dimension s generated by $\overline{E_1}$. Nestedness of the E_n implies $\bigcup_{n=1}^{\infty} \overline{E_n} \subseteq S$. The geometric idea underlying the construction of c^*, d^*, e^* is as follows. We look for a point $c^* \in \bigcap_{n=1}^{\infty} \overline{E_n}$ such that there is a direction d^* leading from c^* into $\overline{E_n}$ for each $n \in \mathbb{N}$. This d^* is found by considering iteratively facets of decreasing dimension of certain polyhedra contained in suitable subsets of $E_n \cap S$. The vector e^* then points towards the interior E_n^0 of E_n in S. Thus moving a short enough step from c^* into the direction d^* and subsequently towards e^* a suitable choice for the machine constants for inputs of dimension at most n is found.

Let $P_n^{(s)}$ be a closed s-dimensional polyhedron in E_n and let $F_n^{(s-1)}$ denote an $s-1$-dimensional facet of $P_n^{(s)}$. Let $e_n^{(s-1)}$ be a normal vector of this facet pointing to $P_n^{(s)}$. Thus $F_n^{(s-1)}$ together with $e_n^{(s-1)}$ generate S. The sequence $\{e_n^{(s-1)}\}_n$ of vectors of length 1 in $\mathbb{R}^k$ is bounded and thus has a condensation point $e^{(s-1)} \in \mathbb{R}^k$. Let $S^{(s-1)}$ denote the $s-1$-dimensional affine subspace defined as orthogonal complement of $e^{(s-1)}$ in S. Without loss of generality suppose that $e^{(s-1)}$ points for each n from $S^{(s-1)}$ towards a side where parts of E_n are located. Due to nestedness of the E_n and the fact that $S^{(s-1)} \cap \overline{E_n}$ is $s-1$-dimensional for all n at least one among the vectors $e^{(s-1)}$ and $-e^{(s-1)}$ must satisfy this condition. Then for all n and for all points x in the interior of $S^{(s-1)} \cap \overline{E_n}$ (the interior with respect to $S^{(s-1)}$) the point $x + \mu \cdot e^{(s-1)}$ for sufficiently small $\mu > 0$ lies in E_n. The vector e^* in the statement is chosen to be $e^{(s-1)}$.

We repeat the above argument iteratively, now starting with $S^{(s-1)}$ instead of S and considering a family of the $s-1$-dimensional polyhedra $P_n^{(s-1)} \subset S^{(s-1)} \cap \overline{E_n}$ as well as their $s-2$-dimensional facets $F_n^{(s-2)}$. This way affine subspaces $S^{(s-2)}, \ldots, S^{(1)}$ and corresponding vectors $e^{(s-2)}, \ldots, e^{(1)} \in \mathbb{R}^k$ are obtained such that $e^{(i)}$ is orthogonal to $S^{(i)}$, each $S^{(i)} \cap \overline{E_n}$ is a polyhedron of dimension i and for sufficiently small $\mu > 0$ and a point x in the interior (with respect to $S^{(i)}$) of $S^{(i)} \cap \overline{E_n}$ the point $x + \mu \cdot e^*$ belongs to E_n. The final step in the construction defines c^* and d^*. Since $S^{(1)} \cap \overline{E_n}$ is a closed 1-dimensional polyhedron for all $n \in \mathbb{N}$ and since $S^{(1)} \cap \overline{E_{n+1}} \subseteq S^{(1)} \cap \overline{E_n}$ there is a point $c^* \in \bigcap_{n \geqslant 1} S^{(1)} \cap \overline{E_n}$. Define d^* such that it points from c^* into $S^{(1)} \cap \overline{E_n}$, i.e. for all $n \in \mathbb{N}$ and sufficiently small $\mu > 0$ it is $c^* + \mu \cdot d^* \in \overline{E_n}$.

Altogether we have shown the existence of points $c^*, d^*, e^* \in \mathbb{R}^k$ satisfying

$$\forall n \in \mathbb{N}\ \exists \epsilon_1 > 0\ \forall \mu_1 \in (0,\epsilon_1)\ \exists \epsilon_2 > 0\ \forall \mu_2 \in (0,\epsilon_2):\quad c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^* \in E_n. \qquad \square$$

Note that in the above construction one cannot stop after having found $S^{(s-1)}$ and $e^{(s-1)}$. It is in general not the case that choosing a point c in $S^{(s-1)} \cap \bigcap_{n \geqslant 1} \overline{E_n}$ and an arbitrary direction e from c into $S^{(s-1)}$ will result in the required property. We do not know how the sequence of the $\overline{E_n}$'s might contract.

Note as well that since we cannot determine how small ϵ_1 and ϵ_2 have to be chosen for given n, the above construction does not give an obvious efficient way to compute points in E_n.

3.2. Efficient elimination of ∃∀∃∀ quantifiers

In order to show $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const} = \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ we are left with deciding the following question: Let $M(\bullet, c)$ be a basic machine in the restricted model using k machine constants and witnessing $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$. Given $x \in \mathbb{R}^n$ what is M's result on $M(x, c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^*)$ for sufficiently small μ_1, μ_2? Here, we have to obey the order in which μ_1 and μ_2 tend to 0. That is for all sufficiently small $\mu_1 > 0$ M has to work the same way when μ_2 tends to 0.

Answering this question efficiently is possible due to the linear structure in which the coefficients of a restricted machine occur.

Theorem 8. *Let M be a restricted basic machine running within a polynomial time bound $t(n)$ and using k machine constants. Suppose there are points $c^*, d^*, e^* \in \mathbb{R}^k$ such that for all $n \in \mathbb{N}$ the following condition is satisfied: $\exists \epsilon_1 > 0\ \forall \mu_1 \in (0,\epsilon_1)\ \exists \epsilon_2 > 0\ \forall \mu_2 \in (0,\epsilon_2)$ $M(x, c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^*)$ decides correctly the n-dimensional part $L \cap \mathbb{R}^{\leqslant n}$ of a language L. Then $L \in \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$.*

Proof. Let M be as in the statement, $x \in \mathbb{R}^n$ an input. A polynomial time restricted machine M' for L works as follows. The constants which M' uses are c^*, d^*, and e^*. It tries to simulate M on x by computing, independently of the constants which

M uses, the form of each test M performs. Then M' evaluates the result of such a test assuming that M uses as its constants $c^* + \mu_1 \cdot d^* + \mu_2 \cdot e^*$ for small enough μ_1, μ_2. More precisely, any test which M performs when using as constants a vector $c \in \mathbb{R}^k$ has the form

$$\sum_{i=1}^{k} p_i(x) \cdot c_i + q(x) \geqslant 0? \tag{$*$}$$

Here, the p_i and q are polynomials in the input x. They can be computed by M' without use of constants by simulating M symbolically, i.e. without actually performing those operations involving components of c. Machine M' only keeps track of which coefficient a c_i finally has in the representation $(*)$. Using constants c^*, d^*, e^* machine M' can as well compute the terms

$$T_1 := \sum_{i=1}^{k} p_i(x) \cdot c_i^* + q(x), \qquad T_2 := \sum_{i=1}^{k} p_i(x) \cdot d_i^*, \qquad T_3 := \sum_{i=1}^{k} p_i(x) \cdot e_i^*.$$

For deciding the result of the above test for M and suitable μ_i the new machine tests one after another whether $T_1 = 0$, $T_2 = 0$ and $T_3 = 0$. The sign of the first T_i for which the test gives a result $\neq 0$ gives as well the answer for M's behavior. If all $T_i = 0$, then M follows the 'yes' branch. In the same way M' simulates the entire computation of M. Clearly, the running time of M' is linear in the running time of M. $\square$

Given the results of this and the previous section the two main results Theorem 1 and Theorem 2 follow: The equality $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const} = \mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$ is obtained by applying Theorems 7 and 8. And the analogue of Ladner's theorem then follows from Theorems 1 and 6.

4. Conclusions

We have extended the list of computational models for which Ladner's theorem holds by a new variant of the BSS model over the reals. The latter allows to compute as in the full model with input values but has limited access to the machine constants only. Real constants can be used freely in additions and subtractions, but must not be multiplied with each other. This model seems closer to the full BSS model than the linear variants. It has as well solvability of systems of polynomial equations as $\mathrm{NP}_{\mathbb{R}}^{\mathrm{rc}}$-complete problem and its P versus NP question seems not easy to be solved either.

The proof of Ladner's result in this model once more relies on showing that the class $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ is equal to $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}$. Establishing this equality however is much more involved than for the additive BSS model over $\mathbb{R}$ or the BSS model over $\mathbb{C}$. It relies on the topological structure of the set of suitable constants.

Techniques like ours which allow to replace in certain situations machine constants by others are important in many arguments concerning real number complexity theory. It seems interesting to study whether similar ideas might help for dealing with the question in the full real number BSS model as well. A promising idea could be to consider a new variant of Michaux' class $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$ which for example requires by definition convexity of the sets E_n of suitable constants. However, then it is unclear whether $\mathrm{P}_{\mathbb{R}}$ is captured by this new non-uniform class. More generally, the diagonalization technique used for $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$ in [1] and for $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ above allows some degree of freedom as to how to define $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$. This means that we can put some additional conditions onto the set of constants that we allow for a fixed dimension to work. To make the diagonalization work there are basically two aspects to take into account. First, the resulting class has to contain $\mathrm{P}_{\mathbb{R}}$. Secondly, the conditions we pose for the constants have to be semi-algebraically definable without additional real constants. An example of the latter occurs in our definition of $\mathrm{P}_{\mathbb{R}}^{\mathrm{rc}}/\mathrm{const}$ in that we require the constants to be bounded by 1 in absolute value. Other properties are conceivable and might lead to new results.

Another obvious attempt is to use the above technique for replacement of constants as well in the full model and Michaux' original class $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$. For a problem L in $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$ the topological structure of the set of suitable constants is more complicated since now each branch results in a (potentially infinite) intersection of semi-algebraic conditions. Then one has to study how the topology of the sets $\bigcap_{i=1}^{N} E_i$ evolves for increasing N. For example, could one guarantee the existence of say a semi-algebraic limit curve along which one could move from a point c^* into an E_n? In that case, a point on the curve might only be given by a semi-algebraic condition. As consequence, though one would likely not be able to show $\mathrm{P}_{\mathbb{R}}/\mathrm{const} \subseteq \mathrm{P}_{\mathbb{R}}$ maybe at least a weaker uniform version of Ladner's result could be settled. It seems reasonable to first analyze the problem in the linear BSS model then.

Finally let us stress that there is at least literally a close resemblance between the quantifier structure as it occurs in Theorem 7 and the exotic quantifiers introduced and studied by Bürgisser and Cucker in [4]. Among the latter we find quantifiers having the meaning 'for sufficiently small $\mu > 0$', thus being similar to the requirements for the directions expressed in the theorem. It might be promising to make this resemblance tighter, for example by studying the relation between some of the complexity classes in [4] defined on base of exotic quantifiers and new variants of the class $\mathrm{P}_{\mathbb{R}}/\mathrm{const}$ in the full real number model.

References

[1] S. Ben-David, K. Meer, C. Michaux, A note on non-complete problems in $NP_{\mathbf{R}}$, J. Complexity 16 (1) (2000) 324–332.
[2] Lenore Blum, Felipe Cucker, Michael Shub, Steve Smale, Complexity and Real Computation, Springer, New York, 1998.
[3] Peter Bürgisser, On the structure of Valiant's complexity classes, in: STACS 98, Paris, 1998, in: Lecture Notes in Comput. Sci., vol. 1373, Springer, Berlin, 1998, pp. 194–204.
[4] Peter Bürgisser, Felipe Cucker, Exotic quantifiers, complexity classes and complete problems, Found. Comput. Math. 7 (2) (2009) 135–170.
[5] Olivier Chapuis, Pascal Koiran, Saturation and stability in the theory of computation over the reals, Ann. Pure Appl. Logic 99 (1–3) (1999) 1–49.
[6] F. Cucker, M. Shub, S. Smale, Separation of complexity classes in Koiran's weak model, in: Selected Papers of the Workshop on Continuous Algorithms and Complexity, Barcelona, 1993, Theoret. Comput. Sci. 133 (1) (1994) 3–14.
[7] Reinhard Diestel, Graph Theory, third edition, Grad. Texts in Math., vol. 173, Springer, Berlin, 2005.
[8] Richard E. Ladner, On the structure of polynomial time reducibility, J. Assoc. Comput. Mach. 22 (1975) 155–171.
[9] Gregorio Malajovich, Klaus Meer, On the structure of $NP_{\mathbb{C}}$, SIAM J. Comput. 28 (1) (1999) 27–35.
[10] Klaus Meer, On Ladner's result for a class of real machines with restricted use of constants, in: Computability in Europe, in: Lecture Notes in Comput. Sci., vol. 5635, Springer, 2009, pp. 352–361.
[11] Christian Michaux, $P \neq NP$ over the nonstandard reals implies $P \neq NP$ over $\mathbf{R}$, Theoret. Comput. Sci. 133 (1) (1994) 95–104.